PCT/EP2004/050217

BUNDESREPUBLIK DEUTSCHLAND

06 MRT 2004

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

PRIORITY DOCUMENT
SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Aktenzeichen: 103 13 409.3

Anmeldetag: 25. März 2003

Anmelder/Inhaber: Continental Teves AG & Co oHG, 60488 Frankfurt/DE

Bezeichnung: Verfahren zum Vermeiden von fehlerhaften Aktuatorzugriffen in einem multifunktionalen elektronischen Gesamtregelungssystem

IPC: G 05 B, B 60 R

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 26. Januar 2004
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

Hintermeier

A 9161
06/00
EDV-L

Continental Teves AG & Co. oHG

24.03.03
GP/BR/KDB/ad
P 10663
A. Kohl
Ch. Kebbel

Verfahren zum Vermeiden von fehlerhaften Aktuatorzugriffen in einem multifunktionalen elektronischen Gesamtregelungssystem

Die Erfindung bezieht sich auf ein Verfahren zum Vermeiden von fehlerhaften Aktuatorzugriffen in einem multifunktionalen elektronischen Gesamtregelungssystem, bei dem die Aktuatorzugriffsanforderungen von verschiedenartigen Systemdiensten ausgehen. Das Verfahren ist insbesondere für Fahrzeugregelungssysteme geeignet.

Es sind bereits komplexe Kraftfahrzeugregelungssysteme bekannt, die mehrere Funktionen, wie Antiblockierschutz (ABS), Anfahrschlupfregelung (ASR), Fahrstabilitätsregelung (ESP), elektrische Überlagerungslenkung, Bremsassistent, System- oder Komponentendiagnose usw. vereinen. Es besteht der Wunsch, diese und weitere Funktionen und Hilfsfunktionen, wie Überwachung, Fehlersignalisierung, Reifendrucküberwachung etc., ebenfalls mit Hilfe eines gemeinsamen elektronischen Systems zu steuern. Die verschiedenen Funktionen und Hilfsfunktionen werden dabei zum großen Teil mit Hilfe derselben Aktuatoren, wie Druckregelventilen, Hydraulikpumpen, Warnlampen etc., ausgeführt oder vorbereitet. Die Zugriffe zu den einzelnen Aktuatoren können dabei durchaus gleichzeitig erfolgen. Dies führt verständlicher Weise zu Konflikten. Ein Zugriff zu einem Aktuator durch ein Regelungssystem

oder einen Regelungsbefehl untergeordneter Bedeutung anstelle eines z.B. aus Sicherheitsgründen momentan wichtigeren Befehls muss verhindert werden.

Der vorliegenden Erfindung liegt daher die Aufgabe zugrunde sicherzustellen, dass in einem komplexen System der vorgenannten Art bei konkurrierenden Aktuatorzugriffsanforderungen kein "fehlerhafter" , nicht berechtigter Zugriff zu einem Aktuator erfolgt. "fehlerhaft" ist dabei ein Zugriff durch eine Anforderung, die momentan unerwünscht ist, weil eine Arbitrierungsart gefordert wird, die in der aktuellen Betriebsphase nicht zulässig ist (z.B. eine Diagnosemaßnahme während der Fahrt) oder aus zahlreichen anderen Gründen.

Es hat sich herausgestellt, dass diese Aufgabe durch das im Anspruch 1 beschriebene Verfahren gelöst werden kann, dessen Besonderheit darin besteht, dass in das System eine Rechteverwaltung, die bei einer Aktuatorzugriffsanforderung die Berechtigung des Systemdienstes zur Änderung der momentanen Betriebsart des Gesamtregelungssystems feststellt, eine Betriebsartensteuerung und eine Zugriffsverwaltung eingefügt werden, dass die Rechteverwaltung bei einer Zugriffsanforderung durch einen Systemdienst unter Berücksichtigung der momentanen Gesamtbetriebsart des Gesamtregelungssystems eine Einstellung oder einen Wechsel der Betriebsart nach vorgegebenen Regeln herbeiführt und die aktuelle Betriebsart der Zugriffsverwaltung meldet, und dass die Zugriffsverwaltung in Abhängigkeit von der gemeldeten Gesamtbetriebsart eine Aktuatorbetätigung nur durch den "berechtigten" Systemdienst zulässt und die Aktuatorzugriffsanforderungen der Systemdienste nach vorgegebenen Arbitrationsregeln verarbeitet.

Erfindungsgemäß wird also in das elektronische Steuersystem eines multifunktionalen Gesamtregelungssystems eine zusätzliche Rechte- und Zugriffsverwaltung integriert, die dazu führt, dass nur die in der jeweiligen Betriebsart "erwünschten", festen vorgegebenen Regeln entsprechende Zugriffsanforderungen der verschiedenen oder verschiedenartigem Systemdienste zum Aktuator durchgelassen werden. Den z.B. aus Sicherheitsgründen vorzuziehenden Aktionen wird von der Zugriffsverwaltung Vorrang oder Priorität eingeräumt.

Durch die erfindungsgemäße Rechte- und Zugriffsverwaltung wird es möglich, Basisfunktionen und Hilfs- oder Fremdfunktionen in einem System zu integrieren, ohne die Basisfunktionen zu gefährden. Durch die Rechte- und Zugriffsverwaltung wird verhindert, dass z.B. durch einen "fehlerhaften", nicht berechtigten Zugriff auf einen Aktuator eine Bremsbetätigungsanforderung, die aus Sicherheitsgründen Vorrang haben muss, nicht mehr durchgeschaltet werden kann. Die Erfindung macht es also erst möglich, dass zahlreiche wichtigere und - je nach Situation bzw. Betriebsart - weniger wichtige Funktionen integriert werden können.

Nach einem vorteilhaften Ausführungsbeispiel des erfindungsgemäßen Verfahrens werden die Aktuatorzugriffanforderungen der Systemdienste in einem Speicher erfasst und nach Arbitrationsarten getrennt zur Zugriffsverwaltung weitergeleitet.

Eine besonders vorteilhafte Ausführungsart der Erfindung besteht, dass die zu einem Aktuator durchgelassene, von einem Systemdienst ausgehende Aktuatorzugriffsanforderung durch

zweistufige Arbitration, nämlich durch eine "vertikale" und eine "horizontale" Arbitration, bestimmt wird.

Nach einem weiteren Ausführungsbeispiel der Erfindung werden in der Zugriffsverwaltung in einem ersten Schritt die nicht berechtigten Zugriffsanforderungen in Abhängigkeit von der gemeldeten, aktuellen Gesamtbetriebsart ermittelt, eliminiert oder zurückgewiesen werden. In einem zweiten Schritt wird durch vertikale Arbitration eine Bewertung und Auswahl der berechtigten Zugriffsanforderungen nach vorgegebener Rangfolge der Arbitrationsarten durchgeführt, wobei einem "Stromsignal" höhere Priorität als einem "Drucksignal" und einem "EIN/AUS-Signal" höhere Priorität als einem Stromsignal zugemessen werden. Schließlich erfolgt in einem dritten Schritt durch horizontale Arbitration eine Bewertung und Auswahl der in dem zweiten Schritt ermittelten Zugriffsanforderungen nach Priorität des Signals, mit dem der ausgewählte Systemdienst den Aktuator ansteuern will.

Es ist zweckmäßig, die Rechte der Systemdienste zur Änderung der Betriebsart in einem Festwertspeicher, auf den die Rechteverwaltung Zugriff hat, z.B. in Form einer Tabelle, festzuhalten.

Wird das erfindungsgemäße Verfahren bei einem Gesamtregelungssystem für Kraftfahrzeuge angewendet, das als Basissystem eine Bremsanlage (EHB, EMB) enthält, werden als Systemdienste, von denen Aktuatorzugriffsanforderungen ausgehen, die Basisbremsfunktionen (BBF), Radschlupfregelungsfunktionen (wie ABS, ASR(TCS),ESP), Diagnosefunktionen (DIAG), Motorpumpenregelungensysteme (MPA) und Schnittstellen (BUS)

erfasst und durch die Rechteverwaltung in Verbindung mit der Zugriffsverwaltung kontrolliert.

Es können noch weitere Systemdienste, wie "Fremdsoftware", (CSW) "Lenkungsfunktionen" (Lenk) etc., in das Gesamtsystem integriert werden.

Bei einem Gesamtregelungssystem für Kraftfahrzeuge wird vorteilhafter Weise in der Betriebartensteuerung zumindest zwischen den Betriebsarten "Normalbetrieb", der sich nach Beendigung der Startphase beim Ausbleiben einer Fehlermeldung einstellt, der Betriebsart "Startphase", die z.B. bis zum Ablauf einer vorgegebenen Zeitspanne, bis zum erstmaligem Erreichen einer Mindestgeschwindigkeit und/oder bis zum Abschluss von anfänglichen Prüfroutinen gilt, der Betriebsart "Diagnose", der Betriebsart "Fremdsoftware", die bei einer Aktuatorzugriffsanforderung durch ein Fremd- oder Hilfssystem ausgelöst wird, und der Betriebsart "Failsafe", die auf das Vorliegen einer Fehlermeldung hinweist, unterschieden.

Weitere Merkmale, Vorteile und Anwendungsmöglichkeiten der Erfindung gehen aus der folgenden Beschreibung von Einzelheiten eines Ausführungsbeispiels anhand der beigefügten Zeichnung hervor. Es zeigen

Fig. 1 in schematischer Darstellung Funktionselemente eines elektronischen Gesamtregelungssystems zur Ausführung des erfindungsgemäßen Verfahrens und

Fig. 2 ebenfalls in schematischer Darstellung einen Teil des Gesamtregelungssystems nach Fig. 1 zur Veranschaulichung der Funktionsweise der Zugriffsverwaltung.

Das im folgenden als vereinfachtes Beispiel beschriebene Gesamtregelungssystem ist für ein Kraftfahrzeug mit einer komplexen Bremsanlage, wie einem elektrohydraulischen Bremsensystem (EHB) vorgesehen, das mit Systemen und Funktionen unterschiedlicher Art, wie Bremsassistent, Geschwindigkeits- oder Abstandregelungssystemen, Diagnosesystemen, Lenksystemen (z.B. Überlagerungslenkung) etc. zusammenarbeiten kann. Das Bremsensystem, einschließlich der zugehörigen Regelungssysteme und -funktionen ABS, ASR, ESP etc. wird als Basissystem betrachtet, die übrigen Systeme oder Funktionen als Fremd- oder Hilfssysteme.

In Fig. 1 werden die Dienste, von denen Aktuatorzugriffsanforderungen ausgehen, die nach dem erfindungsgemäßen Verfahren "verwaltet", d.h. auf ihre Berechtigung geprüft werden, durch einen Funktionsblock 1 symbolisch dargestellt. In dem hier beschriebenen Ausführungsbeispiel nach der Erfindung handelt es sich, wie in 1 angedeutet, im wesentlichen um die folgende Dienste:

BBF bezeichnet die Basisbremsfunktion, die z.B. bei Brake-By-Wire-Systemen (EHB; EMB) auch in Standardsituationen elektronische Steuerung verlangt;

ABS, ASR(TCS), ESP sind unter diesen Abkürzungen bekannte Regelungsfunktionen;

DIAG bezeichnet Diagnosefunktionen;

MPA ist die Bezeichnung für ein Motorpumpenaggregat, vom dem ebenfalls Aktuatorzugriffsanforderungen ausgehen;

CSW symbolisiert Fremd- oder Hilfssysteme (CSW = Customer Software);

BUS bezeichnet eine Schnittstelle, wie CAN-Bus, über die u.a. auch Zugriffsanforderungen von Zubehörfunktionen oder von Fremdsystemen (CSW) geleitet werden;

Lenk bezeichnet Lenksysteme, wie Überlagerungslenkungen.

Zugriffsanforderungen von Abstandsregelungssystemen (ACC), Geschwindigkeitsregelungssystemen (Tempomat) etc. können ebenfalls über den Systemdienst "BUS", über die Schnittstelle CSW oder über einen weiteren Systemdienst mit eigener Identität (ID) in das Gesamtregelungssystem integriert werden.

Die von den Systemdiensten 1 ausgehenden Aktuatorzugriffsanforderungen werden in einer Rechteverwaltung 2 auf Zulässigkeit oder Berechtigung in der aktuellen Situation, d.h. in der momentanen Betriebsart (Gesamtbetriebsart), überprüft. Hierzu dient eine Rückmeldung aus einer Betriebsartensteuerung 3.

Jeder Dienst wird durch seine ID eindeutig erkannt. Als Betriebsarten, die unterschiedliche Reaktionen verlangen, sind beispielsweise die folgenden von Bedeutung:

"Normal" "Normal-Betrieb" ist z.B. nach längerer Betriebszeit eines Kraftfahrzeugs ohne Fehlermeldung gegeben;

"Start-Phase" gilt z.B. solange die einzelnen Systeme noch nicht voll in Funktion sind oder Routineüberprüfungen noch nicht abgeschlossen sind;

"Diagnose" diese Betriebsart herrscht z.B. in der Werkstatt oder in der Startphase des KFZ während des Ablaufs von Prüfroutinen;

"CSW" Fremdsoftware: diese Betriebsart wird z.B. eingestellt, wenn die ID des den Zugriff anfordernden Systemdienstes erkennen lässt, dass die Anforderung nicht von einer Basisfunktion, sondern von einer Zubehör- bzw. Hilfsfunktion oder "Fremdfunktion" stammt;

"Failsafe" im System wurde ein Fehler erkannt, der Betriebseinschränkungen zur Folge hat.

Die Regeln zur Beurteilung der "Berechtigung" in Abhängigkeit von dem identifizierten Systemdienst und von der aktuellen Betriebsart (Gesamtbetriebsart) sind fest vorgegeben. Die Regeln sind, wie Fig. 1 zeigt, in dem beschriebenen Ausführungsbeispiel der Erfindung in einem Festwertspeicher 3, z.B. tabellarisch, festgehalten.

Die Zugriffsanforderung des jeweiligen Systemdienstes 1 wird von der Rechteverwaltung 2 sofort abgelehnt oder ignoriert, wenn in der aktuellen Gesamtbetriebsart keine Berechtigung zu der Aktuatorzugriffsanforderung gegeben ist. Wenn die Anforderung in der aktuellen Betriebsart "berechtigt" ist, wird durch die Betriebsartensteuerung 4, falls erforderlich, ein Wechsel der Betriebsart des Gesamtregelungssystems herbeigeführt. Die aktuelle Betriebsart wird einer Zugriffsverwaltung 6 gemeldet; außerdem erfolgt eine Rückmeldung an die Rechteverwaltung 2.

Die Aktuatorzugriffsanforderungen der einzelnen Systemdienste 1 werden über die Signalwege SD1 bis SDn, gleichzeitig mit der Rechteüberprüfung in der Rechteverwaltung 2, über einen Zwischenspeicher 5 der Zugriffsverwaltung 6 zugeführt, die nach vorgegebenen Regeln durch Arbitration gesteuert

festlegt, welche Aktuatorzugriffsanforderung der Systemdienste 1 in der aktuellen Betriebsart tatsächlich bis zu einen Aktuator 7 durchgelassen wird. Alle anderen Anforderungen werden ignoriert oder wegen "fehlender Berechtigung" zurückgewiesen; die Akzeptanz und/oder die "Ablehnung" der Anforderung wird den Systemdiensten 1 zurückgemeldet.

Wie Fig. 2 veranschaulicht, werden in dem Zwischenspeicher 5 die Aktuatorzugriffsanforderungen nach Arbitrationsarten, d.h. nach Signalen gleicher physikalischer Einheit (hier: Druck "p", Strom "I" oder EIN/AUS-Signal "E/A"), sortiert und zur Zugriffsverwaltung weitergeleitet.

In der Zugriffsverwaltung 6 werden in einem ersten Schritt die in der aktuellen Gesamtbetriebart "nicht berechtigten" Anforderungen zurückgewiesen oder eliminiert. Sodann findet eine zweistufige Arbitration der verbliebenen Aktuatorzugriffsanforderungen statt. In einer ersten Stufe, symbolisiert durch einen Block 8 in Fig. 2, werden die "berechtigten" Anforderungen nach vorgegebener Rangfolge oder Prioritätsrang der einzelnen Arbitrationsarten bewertet; dies wird als "vertikale" Arbitration bezeichnet.

Anschließend wird in einem zweiten Schritt oder einer zweiten Stufe 9 durch "horizontale" Arbitration eine Bewertung der verbleibenden Anforderungen gleicher Arbitrationsart getroffen und festgelegt, welche der Aktuatorzugriffsanforderungen tatsächlich bis zu dem Aktuator 7 durchgelassen wird. Symbolisiert durch einen Umschalter 10 wird das Ausgangssignal der Stufe 9 - je nach Arbitrationsart, d.h. hier "Druck", "Strom" oder "EIN/AUS"-Signal - direkt oder nach Weiterver-

arbeitung in einem Druckregler 11 und/oder in einem Stromregler 12 zu dem Aktuator 6 weitergeleitet. 9

In dem hier beschriebenen Ausführungsbeispiel der Erfindung ist der Aktuator 7 eine Spule, z.B. die Ventilspule eines Bremsdrucksteuerventils. Ein Befehl oder Signal der Einheit oder Dimension "EIN/AUS" führt unmittelbar zur Reaktion des Ventils. Dem "EIN/AUS"-Signal wird daher im Sinne der horizontalen Arbitration die "höchste" Priorität eingeräumt. Ein Signal der Einheit oder Dimension "Strom" muss dagegen zunächst in einem Stromregler 12 (siehe Fig. 2) ausgewertet und in einen "EIN/AUS"-Befehl umgewandelt werden. Eine Druckänderungsanforderung, also ein Signal der Dimension "Druck", muss zunächst in einem Druckregler 11 in eine Stromänderungsanforderung und danach mit Hilfe des Stromreglers 12 in ein Aktuatorbetätigungssignal bzw. in ein "EIN/AUS"-Signal gewandelt werden. Ein Signals der Dimension "Strom" genießt daher im vorliegenden Ausführungsbeispiel eine höhere Priorität als ein Signal der Dimension "Druck". Bei konkurrierenden Signalen der Dimension "Druck", "Strom" und "EIN/AUS" gelangt das E/A-Signal zur Ausführung; fehlt ein E/A-Signal, wird das Strom-Signal vorgezogen.

Die Zugriffsverwaltung 6 selektiert die Aktuatorzugriffsanforderungen nach vorgegebenen Regeln in Abhängigkeit von der aktuellen Betriebsart. Beispielsweise sind in der Betriebsart "Normal" nur Druck-Sollwertanforderungen "rechtmäßig" und werden ausgewertet; andere Anforderungen werden von der Zugriffsverwaltung 6 zurückgewiesen oder ignoriert. In der Betriebsart "Fremdsoftware" (CSW) sind nur Stellbefehle bzw. Aktuatorzugriffsanforderungen in Form von Drucksignalen erlaubt. In der Betriebsart "Diagnose" sind Stellbefehle in

Form von Stromsignalen oder Ventil-Schaltbefehlen, nicht jedoch von Drucksignalen zulässig. In der Betriebsart "Failsafe" sind nur Aktuatoranforderungen, die von dem Kernsystem ausgehen, zu dem vor allem die sicherheitskritischen Systemdienste gehören, nicht jedoch Aktuatoranforderungen von Zubehörsystemen, Hilfssystemen oder Fremdsystemen (CSW) "rechtmäßig".

Dies sind nur relativ einfache Beispiele. Eine Vielzahl weiterer Vorgaben lässt sich mit Hilfe der Zugriffsverwaltung 6 in Verbindung mit der Rechteverwaltung 2 (3) realisieren.

Patentansprüche:

1. Verfahren zum Vermeiden von fehlerhaften Aktuatorzugriffen in einem multifunktionalen elektronischen Gesamtregelungssystem, bei dem die Aktuatorzugriffsanforderungen von verschiedenen oder verschiedenartigen Systemdiensten (1) ausgehen, dadurch **gekennzeichnet**, dass in das System eine Rechteverwaltung (2), die bei einer Aktuatorzugriffsanforderung die Berechtigung des Systemdienstes (1) zur Änderung der momentanen Betriebsart des Gesamtregelungssystems feststellt, eine Betriebsartensteuerung (4) und eine Zugriffsverwaltung (6) eingefügt werden, dass die Rechteverwaltung (2) bei einer Zugriffsanforderung durch einen Systemdienst (1) unter Berücksichtigung der momentanen Gesamtbetriebsart des Gesamtregelungssystems eine Einstellung oder einen Wechsel der Betriebsart nach vorgegebenen Regeln herbeiführt und die aktuelle Betriebsart der Zugriffsverwaltung (6) meldet, und dass die Zugriffsverwaltung (6) in Abhängigkeit von der gemeldeten Gesamtbetriebsart eine Aktuatorbetätigung nur durch den "berechtigten" Systemdienst (1) zulässt und die Aktuatorzugriffsanforderungen der Systemdienste (1) nach vorgegebenen Arbitrationsregeln verarbeitet.

2. Verfahren nach Anspruch 1, dadurch **gekennzeichnet**, dass die Aktuatorzugriffanforderungen der Systemdienste (1) in einem Speicher (5) erfasst und nach Arbitrationsarten sortiert zur Zugriffsverwaltung (6) weitergeleitet werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch **gekennzeichnet**, dass die zu einem Aktuator (7) durchgelassene, von einem Systemdienst (1) ausgehende Aktuatorzugriffsanforderung durch zweistufige Arbitration, nämlich durch eine "vertikale" und eine "horizontale" Arbitration, bestimmt wird.

4. Verfahren nach einem oder mehreren der Ansprüche 1 bis 3 2, dadurch **gekennzeichnet**, dass in der Zugriffsverwaltung (6) in einem ersten Schritt die nicht berechtigten Zugriffsanforderungen in Abhängigkeit von der gemeldeten, aktuellen Gesamtbetriebsart ermittelt, eliminiert oder zurückgewiesen werden, dass in einem zweiten Schritt durch vertikale Arbitration eine Bewertung und Auswahl der berechtigten Zugriffsanforderungen nach vorgegebener Rangfolge der Arbitrationsarten durchgeführt wird, wobei einem "Stromsignal" höhere Priorität als einem "Drucksignal" und einem "EIN/AUS-Signal" höhere Priorität als einem "Stromsignal" zugemessen wird, und dass in einem dritten Schritt durch horizontale Arbitration eine Bewertung und Auswahl der in dem zweiten Schritt ermittelten Zugriffsanforderungen nach Priorität des Signals für die Ansteuerung des Aktuators (7) erfolgt.

5. Verfahren nach einem oder mehreren der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass die Rechte der Betriebsdienste (1) zur Änderung der Betriebsart in einem Festwertspeicher (3), auf den die Rechteverwaltung (2) Zugriff hat, festgehalten werden.

6. Verfahren nach einem oder mehreren der Ansprüche 1 bis 5, dadurch **gekennzeichnet**, dass bei einem Gesamtregelungssystem für Kraftfahrzeuge, das als Basissystem eine Bremsanlage (EHB,EMB) enthält, als Systemdienste (1), von denen die Aktuatorzugriffsanforderungen ausgehen, die Basisbremsfunktionen (BBF), Radschlupfregelungsfunktionen (wie ABS, ASR(TCS),ESP), Diagnosefunktionen (Diag), Motorpumpenregelungensysteme (MPA) und Schnittstellen (BUS) erfasst und durch die Rechteverwaltung (2) in Verbindung mit der Zugriffsverwaltung (5) kontrolliert werden.

7. Verfahren nach einem oder mehreren der Ansprüche 1 bis 6, dadurch **gekennzeichnet**, dass weitere Systemdienste (1), wie "Fremdsoftware" (CWS), "Lenkungsfunktionen" (Lenk), etc. in das Gesamtsystem integriert werden.

8. Verfahren nach einem oder mehreren der Ansprüche 1 bis 7, dadurch **gekennzeichnet**, dass bei einem Gesamtregelungssystem für Kraftfahrzeuge in der Betriebartensteuerung (3) zumindest zwischen den Betriebsarten "Normalbetrieb", der sich nach Beendigung der Startphase beim Ausbleiben einer Fehlermeldung einstellt, der Betriebsart "Startphase", die z.B. bis zum Ablauf einer vorgegebenen Zeitspanne, bis zum erstmaligem Erreichen einer Mindestgeschwindigkeit und/oder bis zum Abschluss von anfänglichen Prüfroutinen gilt, der Betriebsart "Diagnose", der Betriebsart "Fremdsoftware", die bei einer Aktuatorzugriffsanforderung durch ein Fremd- oder Hilfssystem ausgelöst wird, und der Betriebsart "Failsafe", die auf das Vorliegen einer Fehlermeldung hinweist, unterschieden wird.

Verfahren zum Vermeiden von fehlerhaften Aktuatorzugriffen in einem multifunktionalen elektronischen Gesamtregelungssystem

Zusammenfassung

Bei einem Verfahren zum Vermeiden von fehlerhaften Aktuatorzugriffen in einem multifunktionalen elektronischen Gesamtregelungssystem, bei dem die Aktuatorzugriffsanforderungen von verschiedenartigen Systemdiensten (1) ausgehen, wird in das Gesamtregelungssystem eine Rechteverwaltung (2), die die Berechtigung von Aktuatorzugriffsanforderungen feststellt, eine Betriebsartensteuerung (4) und eine Zugriffsverwaltung (6) integriert. Die Rechteverwaltung (2) führt bei einer Zugriffsanforderung durch einen Systemdienst (1) unter Berücksichtigung der momentanen Betriebsart des Gesamtsystems eine Einstellung oder einen Wechsel der Betriebsart nach vorgegebenen Regeln herbei und meldet die aktuelle Betriebsart der Zugriffsverwaltung (6). Von der Zugriffsverwaltung (5) werden in Abhängigkeit von der gemeldeten Gesamtbetriebsart eine Aktuatorbetätigung durch den "berechtigten" Systemdienst (1) zugelassen und die Aktuatorzugriffsanforderungen der Systemdienste (1) nach vorgegebenen Arbitrationsregeln verarbeitet.

(Fig. 1)

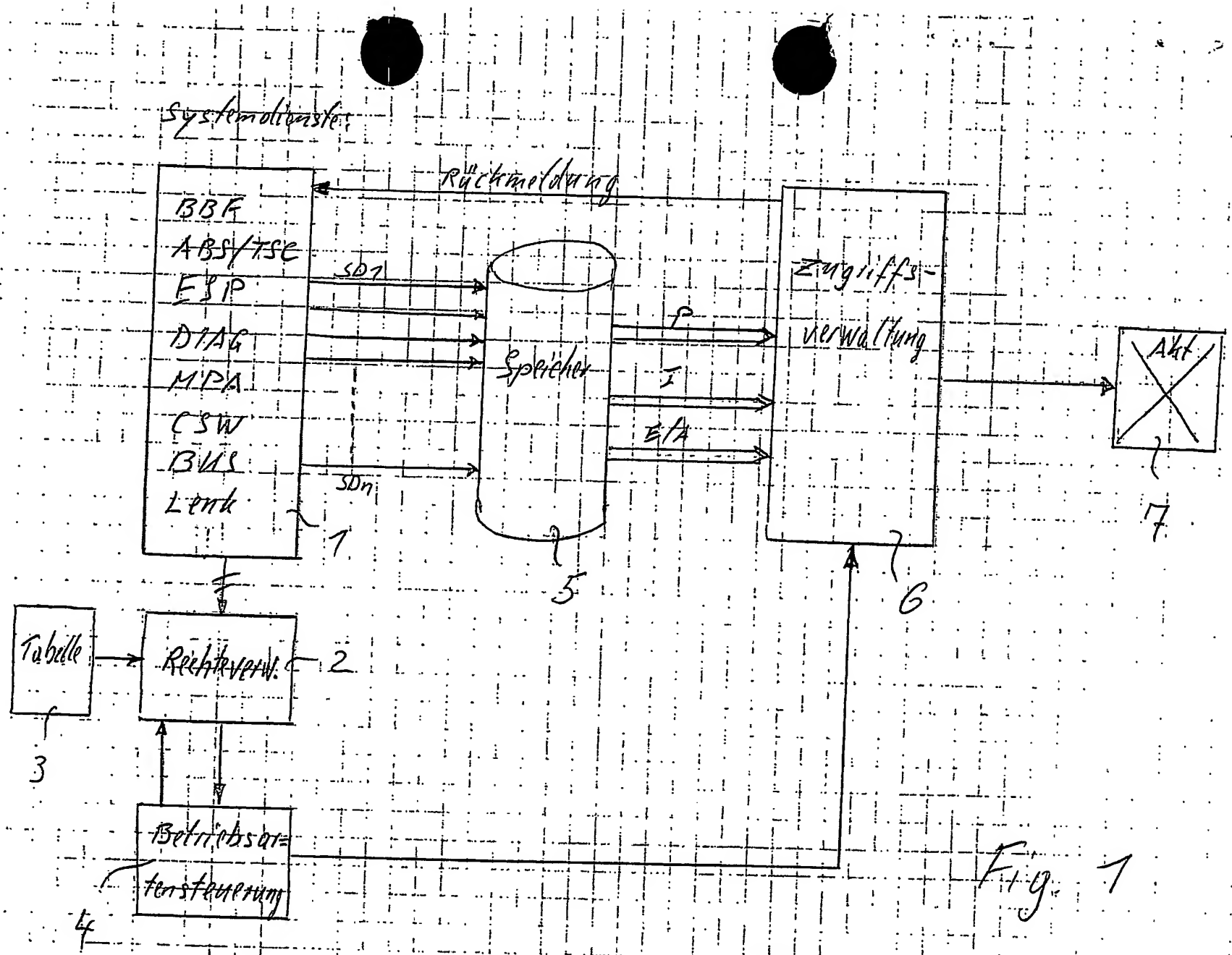
Systemleitstelle
BBF
ABS/TSE
ESP
DIAG
MPA
CSW
BUS
Lenk
1
Rückmeldung
SD1
SDn
Speicher
5
p
I
EPA
Zugriffs-
verwaltung
6
Akt
7
Tabelle
3
Rechteverw.
2
Betriebsar-
tensteuerung
4

Fig. 1

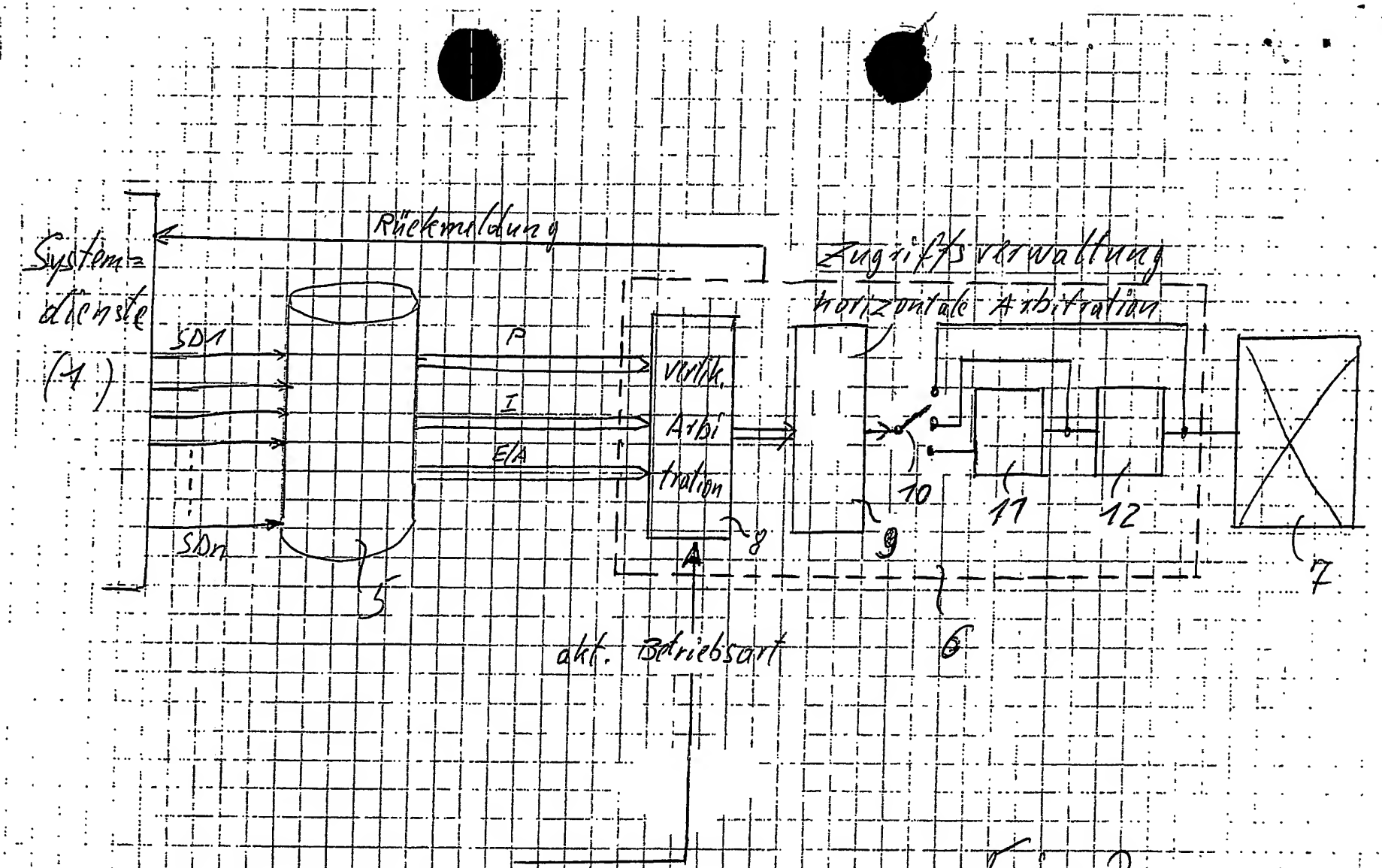
Rückmeldung
Zugriffsverwaltung
horizontale Arbitration
Systemdienste
(4)
SD1
SDn
P
I
E/A
Verifik.
Arbi
tration
A
akt. Betriebsart
5
6
7
8
9
10
11
12

Fig. 2